The official voice of the Air Force Research Laboratory
news@afrl
columns
Summer 2000 Volume II, Issue 2

CIO Tips

Identifying weak passwords controls system access

by Larry Johns, Air Force Communications Agency

Information Assurance begins with some basic requirements. A key element in controlling access to information systems is the requirement for all users to provide some form of identification.

Currently the primary means of doing this is for the user to provide a user ID and password. The password provides the first line of defense for our information systems, and that defense is weakened by poorly constructed passwords.

Air Force requirements for password construction and selection call for passwords to have a minimum number of alpha-numeric characters (upper and lowercase, and at least one special character). System administrators have the availability of password-cracking tools to identify the use of weak passwords. Unfortunately, these tools are not normally used until the password has been in use for some time.

The Air Force is evaluating the use of a password policy enforcement tool that will check passwords as the user initially enters it into the system. Direct feedback is immediately available to the user when the entered password does not meet the requirements, or when the entered password is listed in the tool's accompanying dictionary.

Password cracking tools typically check the password against a dictionary to determine if a match can be found. In some cases the tool will check variations of the dictionary words by adding a letter or number to the beginning or end. The more sophisticated tools use a combination of the dictionary check and then have the capability to complete an exhaustive attack of the password.

Exhaustive attacks involve the submission of as many different password values as possible in the hopes of finding one or more which are valid. The work factor for someone attempting an exhaustive attack is directly related to the number of possible values, which must be tried for each character of the password.

The following illustrates the increased difficulty of cracking passwords when using properly constructed passwords. Using the 26 letters of the English alphabet in any arbitrary arrangement, the number of possible passwords that can be formed using N letters is 26 to the Nth power. The total number of passwords comprises the password space. Thus, using 5-letter passwords, there would be 26 to the 5th possible combinations, which is equal to 11,881,376.

This is fairly easy for a password cracking tool using an exhaustive attack to try all the combinations in a relatively short time. Increasing the password length to eight characters will increase the number of combinations to 208,827,064,576.

This significantly increases the time required for the tool to try all the combinations. The addition of upper case letters, 10 numeric digits, and the possibility of 25 or 30 easily inserted special characters will increase the number of combinations to a gazillion or two (more than I can figure or comprehend). This number will significantly increase the time required for the cracking tool to try all the combinations.

Still, it's not an impossible task given enough time and computing power, but this should be enough to discourage casual intruders. Adding numerics and special characters also makes it more difficult to discover passwords when checked against a dictionary.

Do your part to help protect our information systems by following the rules for properly constructed passwords. **@**